Sind MacOS und Linux wirklich sicherer als Windows? CHIP testet die Sicherheitsdecke aller drei Systeme – und zeigt, wie Sie die Löcher stopfen, die wir gefunden haben.

Von Fabian von Keudell, Jörg Geiger und Daniel Schmid

Windows vs.

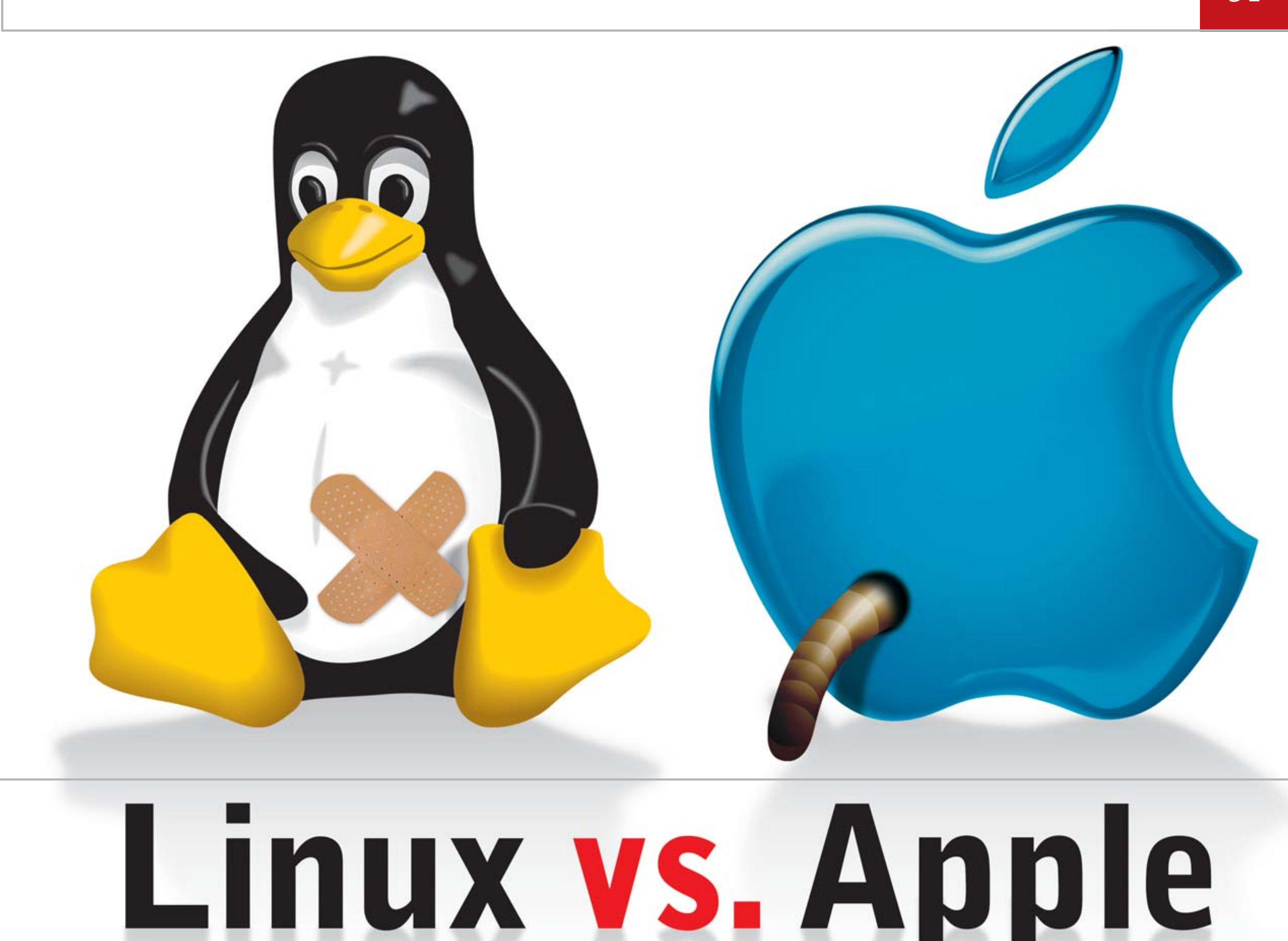
Welches Betriebssystem schützt Ihren PC am besten?

Wir hätten die Kollegen warnen sollen: Immer wenn jemand die Gretchenfrage nach dem sichersten Betriebssystem stellt, löst die Antwort – egal wie sie ausfällt – einen Sturm der Entrüstung aus. So erging es kürzlich auch dem Marktforschungs-Institut Forrester Research (**www.forrester.com**). Ein Jahr lang verglichen die Marktforscher, welche Sicherheitslücken in Windows und verschiedenen Linux-Distributionen auftraten und wie schwerwiegend sie waren. Das Ergebnis: Laut Forrester konnte Microsoft als einziger alle aufgetauchten Lücken schließen – und das auch noch am schnellsten. Die Hersteller der verschiedenen Linux-Derivate wie SuSE, Red Hat, Mandrake und Debian brachten es „nur“ auf rund 99 Prozent – bei längeren Reaktionszeiten. Kaum war die Studie im März 2004 veröffentlicht, hagelte es Kritik von Linux-Distributoren und -Anhängern, die den praktischen Nutzen der Forrester-Methodik in Zweifel zogen.

Wir wissen also, worauf wir uns einlassen – und wagen trotzdem den Vergleich von Äpfeln mit Birnen. Wir schicken jeweils einen Vertreter aus allen drei Welten zum CHIP-TÜV: Windows XP Professional, SuSE Linux (die in Deutschland verbreitetste Distribution) in der Version 9.1 Professional und MacOS X 10.3.3. Alle drei Betriebssysteme durchlaufen die gleichen Prüfstufen.

Stufe 1 – Sicherheit im Internet: Jedes Betriebssystem wird zunächst „out-of-the-box“, also ohne Patches, installiert und dem Online-Check der Sicherheitsprofis von Qualys unterzogen. Dieser Härte-Test klopft das gesamte System auf bekannte Sicherheitslecks ab – derzeit über 3.500 – und teilt sie in fünf Gefahrenstufen ein. Je höher die Einstufung, umso schwerwiegender die Sicherheitslücke.

Anschließend spielen wir alle zum Testzeitpunkt verfügbaren Service Packs, Patches und Updates ein. Falls die Firewall nicht automatisch eingeschaltet ist, aktivieren wir sie manuell. Danach schicken wir alle drei Betriebssysteme nochmals durch den Lücken-Test. Die



Linux vs. Apple

kompletten Vorher-Nachher-Testergebnisse und alle Details zum Testverfahren finden Sie auf **53**.

Alle drei Betriebssysteme bringen außerdem verschiedene Browser mit, die unterschiedlich vorkonfiguriert sind und andere Techniken nutzen. Der von Linux beispielsweise kennt potenziell gefährliche Programmiersprachen wie ActiveX und VBS erst gar nicht. Die als Tor zum Internet besonders anfälligen Browser schicken wir deshalb extra durch einen Browser-Test des Sicherheitsspezialisten scanit (**http://bcheck.scanit.be/bcheck**). Dieser prüft unter anderem, ob Java, JavaScript, ActiveX oder das Umleiten auf andere Domains möglich ist.

Stufe 2 – Alle Lücken manuell stopfen: Sofern trotz Patches und Updates noch Sicherheitslöcher vorhanden sind, egal ob im Browser oder im Betriebssystem, stopfen wir diese selbst; soweit es geht mit Bordmitteln. Wenn diese nicht mehr ausreichen, etwa beim Virenschutz, nennen wir die eingesetzten Tools.

Stufe 3 – Sicherheit auf dem Rechner: Nicht jede Gefahr kommt aus dem Internet. Manchmal sitzt der Spion auch im Büro nebenan. Wir haben deshalb auch die Sicherheitsstrategien der drei Betriebssysteme auf lokaler Ebene genauer unter die Lupe genommen. Wie leicht lassen sich Anmelde-Passwörter aushebeln und wie gut sind sie verschlüsselt? Auch Benutzerverwaltung und Rechtevergabe spielen eine große Rolle: Welche Möglichkeiten haben zum Beispiel Administratoren, Bereiche der Festplatte nur für bestimmte User-Gruppen zugänglich zu machen? Auch benutzerfreundliche Backup-Konzepte tragen zur Datensicherheit bei.

Auf diese Weise zeigt unser 3-Stufen-TÜV also die Stärken und Schwächen der drei Betriebssysteme auf. Und nebenbei erklären wir Ihnen auch noch genau, wie Sie Ihr eigenes Betriebssystem zur Festung ausbauen: für Windows XP ab **52**, für SuSE Linux ab **56** und für MacOS X ab **60**.

→



Leicht hat es Microsoft mit Windows wahrlich nicht, denn täglich geistern Meldungen über neue Sicherheitslücken durchs Web. Was ist dran, am Vorurteil vom unsicheren Betriebssystem – und wie lassen sich die Löcher stopfen?

Logisch, dass das am weitesten verbreitete Betriebssystem die meisten Hacker und Virenprogrammierer anzieht. Denn wer auf eine Windows-Lücke zielt, richtet auch am meisten Schaden an.

Sicherheit im Internet

Out-of-the-box sieht es bei Microsoft zunächst gar nicht gut aus. Über 25 Sicherheitslöcher bringt der Qualys-Check (siehe Kasten rechts) ans Licht, deutlich mehr als SuSE Linux und MacOS X, fünf davon sogar in den höchsten Gefahrenstufen. Doch Microsoft schafft mit dem Service Pack 2 und aktuellen Patches Abhilfe. Nach deren Installation glänzt Windows XP im Lücken-Test mit einer weißen Weste. Ohne aktuelles Update sollten Sie sich mit XP also nicht ins Web wagen.

Sicherheits-Updates installieren

Sie müssen nicht jeden Tag aufs Neue nach Updates suchen, denn die Redmonder stellen sie gesammelt jeden zweiten Dienstag im Monat ins Internet. Von dort laden Sie diese entweder manuell herunter (**http://windowsupdate.microsoft.com**), oder über das in Windows XP integrierte Update-Modul. Sie können diese Automatik so konfigurieren, dass Ihr Betriebssystem alle neuen Updates und Patches selbst holt und installiert.

Aktivierte Firewall inklusive

Erst mit dem Service Pack 2 ist die Firewall automatisch eingeschaltet und schützt damit alle wichtigen Netzwerk- und DFÜ-Verbindungen. Alle ICMP-Pakete, wie beispielsweise den Ping-Befehl, blockt das System komplett. Damit sind Sie fast unsichtbar im Internet unterwegs: Alle Anfragen potenzieller Angreifer an Ihren Rechner leitet XP ins Datennirwana. Hier bedarf es keiner weiteren Einstellungen, alles ist optimal konfiguriert. Und sollte das eine oder andere Programm, etwa eine Tauschbörse, doch einen Port benötigen, fragt Windows automatisch nach, ob es diesen öffnen darf.

Extra Virenschutz installieren

Die Virenautoren haben sich auf Windows eingeschossen: Laut Antiviren-Hersteller Sophos gab es 2003 mehr Viren und Würmer als je zuvor – Tendenz steigend. Da die meisten Virenautoren eine Vielzahl von Rechnern infizieren wollen, bietet sich Windows mit einem Marktanteil von 90 Prozent bei Home Computern geradezu an. Schutz gegen diese Gefahren bietet Windows XP von sich aus allerdings nicht. Diese Aufgaben müssen zusätzliche Programme, in diesem Fall Virenscanner, übernehmen. Dazu eignen sich zwei Programme, die bei In-the-wild-Viren gute Dienste leisten. Das Kaufprogramm AntiVirenKit 2004 Professional von G Data (**www.gdata.de**) schnappt sich jeden Virus dank zweier Scan-Engines. Nachteil: Das Programm erkauft sich den wirksamen →

Service Pack 2: Das neue Sicherheitscenter zeigt, ob Firewall und Updates auf dem neuesten Stand sind.

Sicherheits-Check vom Profi

Um die Sicherheit der Systeme zu testen, hat CHIP in Zusammenarbeit mit den Experten des US-Unternehmens Qualys einen aufwendigen Online-Check durchgeführt. Qualys ist eine der weltweit führenden Sicherheitsfirmen („Best Security Service 2004“, SC Magazine Global Award) und führt pro Quartal rund eine Million Security-Analysen durch. Zu den Referenz-Kunden zählt unter anderem auch die US-Regierung. Für Privatkunden bietet Qualys einen kostenlosen Check an (**https://freescan.qualys.com/**), der sich auf die zehn schwerwiegendsten Sicherheitslöcher bezieht. Die Profi-Checks sind nur für Unternehmen und kosten einen fünfstelligen Betrag.



Online-Check: Qualys spürt Sicherheitslücken im System auf.

In der von uns eingesetzten Enterprise-Version scannt das von Qualys entwickelte Test-Programm den Rechner nach derzeit über 3.500 bekannten und schwerwiegenden Sicherheitslücken.

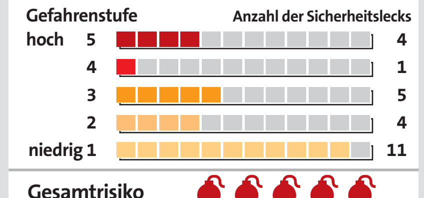
Dabei arbeitet der Test mit sehr großer Genauigkeit, die Fehlerrate beträgt weniger als 0,003 Prozent. Der Sicherheits-Check testet alle relevanten Sicherheitsmerkmale des Rechners im Bereich Internet- und Online-Sicherheit. Die Lücken, die gefunden werden, teilt Qualys in fünf verschiedene Stufen ein: Stufe eins steht für geringste Gefahr, Stufe fünf kennzeichnet schwerwiegende Sicherheitslecks im System. **Info: www.qualys.com**

▶ DIE TESTERGEBNISSE VON QUALYS-GUARD



Windows XP Prof.

▶ **Standard-Installation**



Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	4
	4	1
	3	5
	2	4
niedrig	1	11

Gesamtrisiko

Beim ersten Test zeigt Qualys, dass Windows frisch aus der Packung offen wie ein Scheunentor ist – nicht gerade vertrauenserweckend.

▶ **Installation mit Patches & Updates**

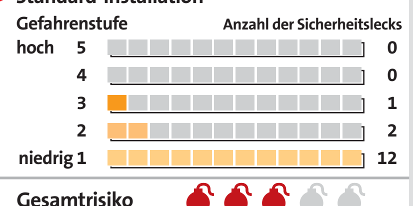
Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	0
	4	0
	3	0
	2	0
niedrig	1	0

Gesamtrisiko

Überraschung: Nachdem Patches und Updates installiert sind, zeigt sich Windows von seiner besten Seite – keine Sicherheitslöcher mehr.

SuSE Linux 9.1 prof.

▶ **Standard-Installation**



Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	0
	4	0
	3	1
	2	2
niedrig	1	12

Gesamtrisiko

Bei SuSE Linux sieht es schon weit besser aus als bei Windows, dennoch ist das Gesamtrisiko immer noch viel zu hoch.

▶ **Installation mit Patches & Updates**

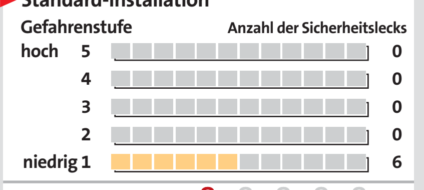
Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	0
	4	0
	3	0
	2	0
niedrig	1	5

Gesamtrisiko

Nach dem Einspielen der Updates und wenigen Mausklicks in den Systemoptionen ist auch SuSE Linux kaum noch angreifbar.

MacOS 10.3.3

▶ **Standard-Installation**



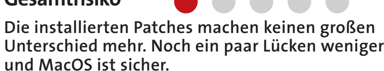
Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	0
	4	0
	3	0
	2	0
niedrig	1	6

Gesamtrisiko

Apple macht keine Kompromisse und riegelt das System schon im Rohzustand nahezu vollständig sicher ab – sehr gut.

▶ **Installation mit Patches & Updates**

Gefahrenstufe		Anzahl der Sicherheitslecks
hoch	5	0
	4	0
	3	0
	2	0
niedrig	1	2



Gesamtrisiko

Die installierten Patches machen keinen großen Unterschied mehr. Noch ein paar Lücken weniger und MacOS ist sicher.

■ Laut Microsoft haben die wenigsten User ein „nacktes“ Windows ohne Sicherheitspatches installiert – und das ist auch gut so. Denn der Qualys-Test fand sage und schreibe 25 Sicherheitslecks, fünf davon sogar in den höchsten Gefahrenstufen. Das Gesamtrisiko des XP-Rechners stufte die Sicherheitsfirma als extrem gefährdet (Stufe 5) ein.

Die von Qualys gefundenen Lücken sind fast allesamt Programmierfehler in bestimmten Windows-Diensten. So zeigt der Test beispielsweise die Sicherheitslücke im Windows Messenger auf, durch den sich Angreifer Zugang zum System verschaffen können. Aber auch zahlreiche Sicherheitslecks durch die berüchtigten Puffer-Überläufe füllen die Mängelliste des Testberichts. Auf diese Lücken greifen auch aktuelle Würmer wie Blaster oder Sasser zurück. Die restlichen Lücken betreffen – wie bei Linux – Dienste, die Informationen über den Rechner preisgeben, etwa ICMP (Internet Control Message Protocol, siehe Glossar **54**), über den der Angreifer unter anderem erfahren kann, welchen Provider Sie verwenden.

Bei so vielen potenziellen Angriffspunkten war die Überraschung nach dem Aufspielen der Updates und des Service Pack 2 groß: Alle Lücken waren geschlossen, keine Informationen über den Rechner von außen mehr sichtbar – ein großer Pluspunkt für Microsoft.

■ Das Vorurteil, Linux sei bombensicher, wird in der Standard-Installation von SuSE relativiert: 15 Lücken findet Qualys, allerdings sind sie bei weitem nicht so riskant wie bei Windows. Das Gesamtrisiko für einen Angriff ordnet Qualys als mittelschwer auf Stufe 3 ein.

Die Lecks betreffen fast nur nach außen hin sichtbare Dienste. Als Angriffspunkte kommen sie nur in Frage, wenn Fehler in diesen Services auftauchen. Die einzige Lücke der Stufe 3 betrifft „Secure Shell“ (SSH), die für eine sichere Verbindung sorgt. Diese OpenSSH-Version enthält einen Bug, der Angreifern Zugang mittels Puffer-Überlauf erlaubt. Zwei weitere Lücken (Stufe 2) betreffen den RPC-Dienst und ICMP-Meldungen. Nach außen hin sichtbar ist ein Portmapper, der RPC-Anfragen an System-Dienste weiterleitet. Schafft es ein Angreifer, ihn zu umgehen und einen Dienst zu starten, kann er Zugang zum Linux-System über einen privilegierten Port bekommen.

Auch das Online-Update ändert daran nichts, erst mit manuell aktivierter Firewall sind 10 Lücken zu. Nach wie vor reagiert SuSE auf Pings: So lässt sich testen, ob ein Rechner erreichbar ist. Gleichzeitig kann mit dem Traceroute-Befehl der Weg der Datenpakete verfolgt werden. Schließlich kann ein Angreifer über eine „Whois“-Abfrage unter **www.ripe.net/perl/whois** ermitteln, bei welchem Provider Sie eingewählt sind.

■ Nach der Standard-Installation von MacOS X meldet Qualys sechs Lücken in der niedrigsten Gefahrenstufe 1, damit ist das Apple-Betriebssystem, zumindest out-of-the-box, das sicherste System.

Vier Lücken gehören in den Bereich Informationsbeschaffung. Wie Linux und Windows lässt auch MacOS ICMP-Anfragen durch, etwa den Ping-Befehl und die Antwort, dass diverse Ports geschlossen sind. Es ist zudem möglich, von außen über den Befehl »traceroute« den Weg eines Datenpakets zu ermitteln und Informationen über den Befehl »whois« zu recherchieren. Im TCP- und UDP-Bereich (siehe Glossar **54**) bemängelt Qualys zwei offene UDP-Ports: 514 (syslog) und 1434 (ms-sql-m). Syslog wird meist bei Netzwerkgeräten (Hubs, Router) eingesetzt, Port 1434 bei der SQL-Authentifizierung. Beide sind jedoch ungefährlich. Insgesamt surft man also mit der Grundkonfiguration bereits entspannt im Web.

Auch hier ändern die Updates nichts, denn sie betreffen unter anderem die Bereiche AFP (Apple Filesharing Protokoll), CUPS (Drucksystem), Mail, IPSec und OpenSSL. Erst nach dem Anpassen der Firewall-Regeln beim internen BSD-Paketfilter „ipfw“ zeigt Qualys nur noch zwei Einträge der Stufe 1 an – etwa die „Reachable Hostlist“. Die zeigt, dass der Mac beim Provider mit einer IP-Adresse und einem DNS-Namen registriert ist.



Gesamtrisiko: Aus Anzahl und Schwere der gefundenen Sicherheitslücken ermittelt Qualys das Gesamtrisiko: von Level 0 (keine rote Bombe) bis Level 5 (5 rote Bomben).

Schutz mit einem extremen Verbrauch an Performance. Schneller geht das kostenlose Tool AntiVir Personal Edition (**www.free-av.de**) vor. Sein Nachteil: Bei Zoo-Viren (künstliche, zu Forschungszwecken programmierte Viren) kann es mit dem Programm AntiVirenKit von G Data nicht mithalten.

Wer ganz auf Nummer sicher gehen will, installiert noch die Software von PivX. Das Tool Qwik-Fix (**www.pivx.com**) geht einen neuen Weg: Es schützt Ihren PC, noch bevor der Hersteller einen Patch herausgebracht hat. Dies erreicht das Tool, indem es die Sicherheitslücke schon vorher behebt, also etwa angegriffene Ports sperrt. PivX ist noch in der Beta-Phase, dafür aber kostenlos.

Browser absichern

Als Browser enthält Windows XP den Internet Explorer 6. Wir fahren den Browser-Check „browser security test" der Firma scanit. Wie beim Qualys-Test zeigt sich: Unbedingt alle Updates installieren! Erst nachdem damit alle Lücken geschlossen waren, meldete der Test keine Angriffspunkte mehr. Auch die Problemkinder ActiveX und VisualBasic-Script stellen jetzt keine Gefahr mehr dar.

Um auch gegen zukünftige Attacken gerüstet zu sein, sollten Sie ActiveX, Java und JavaScript deaktivieren und nur bei Bedarf einschalten. Denn über diesen Dienst richten Angreifer die meisten Schäden an. Dazu öffnen Sie den Internet Explorer und klicken dann im Menü »Extras« auf »Internetoptionen«. Wählen Sie im folgenden Fenster den Reiter »Sicherheit« und drücken Sie auf »Stufe anpassen«. Aktivieren Sie nun vor »ActiveX-Steuerelemente und Plugins ausführen« die Option »Eingabeaufforderung«. Windows XP fragt jetzt bei jedem ActiveX-Element nach, ob der Internet Explorer es ausführen soll. Gleiches gilt für Java, setzen Sie im selben Fenster die Java-Einstellungen auf »Hohe Sicherheit«.

GLOSSAR

»Gefährliche Dienste

Viele Sicherheitslücken betreffen Dienste und Protokolle. Hier die wichtigsten:

ICMP: Das Internet Control Message Protocol transportiert Fehlermeldungen für die Netzwerk-Protokolle IP, UDP und TCP. Die bekannteste ICMP-Meldung ist der Ping-Befehl. Die Vielfalt an ICMP-Meldungen (etwa 20) erlaubt es Angreifern, Informationen über ein System zu sammeln, indem sie die entsprechenden ICMP-Pakete senden.

RPC: Das Remote Procedure Call Protocol startet Funktionen auf anderen Rechnern, etwa beim Remote Computing.

UDP: Das Users Datagram Protocol ist wie TCP ein Kommunikations-Protokoll zwischen Rechnern. Wie TCP kommuniziert UDP über das Internet Protocol (IP).

TCP/IP: Das Internet Protocol (IP) fragmentiert und adressiert Daten und übermittelt sie. Das Transmission Control Protocol (TCP) baut darauf auf, sorgt für die Einsortierung der Pakete in der richtigen Reihenfolge und gewährleistet eine störungsfreie Kommunikation.

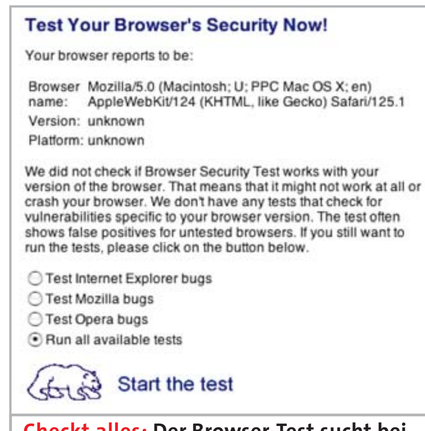
Sicherheit auf dem Rechner

Unter XP können Sie für jeden Anwender einen eigenen Account anlegen. Hier stehen zwei Varianten zur Auswahl: entweder mit allen Rechten und vollem Zugriff auf alle Funktionen des Betriebssystems oder mit eingeschränkten Rechten. User der zweiten Kategorie sollen so zwar auf Ihr System zugreifen, aber keine Software installieren oder Systemeinstellungen ändern können. In der Praxis weisen Benutzerverwaltung und Passwort-Zugang aber einige Lücken auf.

Benutzerkonten absichern

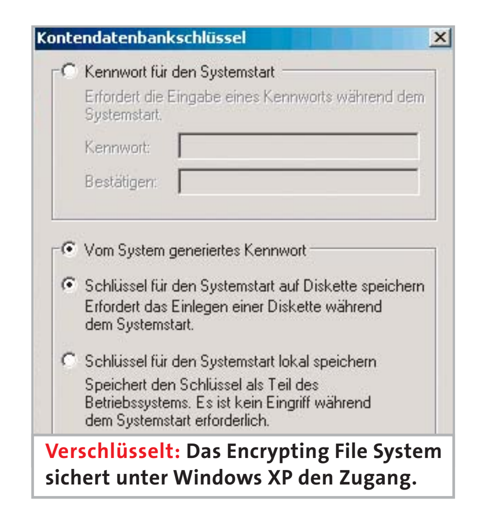
Sie können vor den Start von XP die Abfrage eines BIOS-Passworts setzen. So ist es nur Usern, die das Kennwort wissen, möglich, den PC hochzufahren. Zwar lässt es sich durch Ausbau der Motherboard-Batterie löschen, einen Grundschutz bekommen Sie so jedoch allemal.

Die Kennwörter der Benutzerkonten speichert XP als Hash-Wert (ähnlich einer Quersumme). Wenn Sie ein Passwort eingeben, rechnet Windows es um und vergleicht den errechneten Hash-Wert mit dem gespeicherten. Stimmen sie überein, erhalten Sie Zugriff auf das System. Windows legt diese Werte in der Datei SAM ab, die im Verzeichnis »c:\windows\system32\config« liegt. Doch so sicher wie es klingt, ist das bei weitem nicht: Angreifer, die lokalen Zugriff auf das System haben, können mit ein paar einfachen Tools aus dem Internet den gespeicherten Hash-Wert mit ihrem eigenen Hash-Wert überschreiben und sich so einem Benutzer zuordnen. Dadurch erhalten sie Zugriff auf das System.



Checkt alles: Das Browser-Test sucht bei allen Testkandidaten nach Lücken.

Abhilfe schafft das als sehr sicher geltende EFS (Encrypting File System), mit dem Sie das Dateisystem verschlüsseln können, damit nur berechtigte Benutzer Einblick auf die Festplatte bekommen. Starten Sie »Start | Ausführen | syskey« und drücken Sie [Enter]. Im folgenden Dialog gehen Sie auf »Aktualisieren«. Danach stehen mehrere Optionen zur Verfügung (siehe Bild unten). Der sicherste Weg: Lassen Sie sich vom System ein Passwort generieren und speichern Sie es anschließend auf eine Diskette, die Sie bei jedem Systemstart einlegen müssen.



Verschlüsselt: Das Encrypting File System sichert unter Windows XP den Zugang.

Bei der Benutzerverwaltung gibt es eine weitere Sicherheitslücke. Ändert ein Benutzer sein Kennwort, speichert Windows dieses in zwei Hash-Werte. Beide legt XP wieder in der SAM-Datei ab. Der zweite Wert heißt LMHash (LAN Manager Hash), er ist ein Überbleibsel aus Windows-3.1-Zeiten und wird nur aus Gründen der Kompatibilität angelegt. Hacker haben hier leichtes Spiel, weil LMHash nur Großbuchstaben kennt und sich so die Zahl der möglichen Kennwort-Kombinationen drastisch verringert. Wenn Sie nur XP einsetzen, sollten Sie den zweiten Hash-Wert deshalb deaktivieren. Klicken Sie dazu im Menü »Start« auf »Ausführen«, tippen Sie »regedit« ein und klicken Sie auf »OK«. Gehen Sie dann zum Schlüssel »HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa«. Klicken Sie auf der rechten Seite doppelt auf »nolmhash« und geben Sie unter »Wert« die Ziffer »1« ein. Nach einem Klick auf »OK« beenden Sie den Registry-Editor und starten den PC neu.

Ordner verschlüsseln

Wenn Sie XP Professional nutzen, können Sie NTFS-Ordner codieren. Dazu klicken Sie den Ordner mit der rechten Maustaste an und wählen »Eigenschaften«. Unter »Erweitert« gehen Sie auf »Inhalt verschlüsseln, um Daten zu schützen«. Die Dateien sind nun mit einem 4.096-Bit-Schlüssel gesichert – ein Hacker-Leben würde zum Knacken nicht ausreichen.

Die Verschlüsselung benutzt kein Passwort, sondern ein äußerst sicheres Zertifikat, das auf dem Rechner installiert sein muss und als Schlüssel dient. Nur mit ihm bekommt der Hacker Zugriff auf die Daten. Exportieren Sie deshalb das Zertifikat und löschen Sie es von der Festplatte. Nur so sind die verschlüsselten Daten wirklich sicher. So geht's: Klicken Sie im Menü »Start« auf »Einstellungen«, dann auf »Systemsteuerung« und schließlich doppelt auf »Internetoptionen«. Im Reiter »Inhalte« wählen Sie »Zertifikate«. Klicken Sie auf »Exportieren« und wählen Sie »Weiter«. Die erscheinende Option »Ja, privaten Schlüssel exportieren« aktivieren Sie. Das nächste Fenster können Sie mit »Weiter« überspringen. Nun vergeben Sie ein Kennwort. Als Speicherort →

für den Schlüssel sollten Sie zunächst die Festplatte nutzen. Die weiteren Meldungen bestätigen Sie. Sie finden sich jetzt bei der Zertifikatsübersicht wieder. Wählen Sie »Entfernen« und bestätigen Sie die Sicherheitsabfrage mit »Ja«. Verschieben Sie den exportierten Schlüssel von der Festplatte auf ein externes Speichermedium, etwa Diskette oder Speicher-Stick. Machen Sie aber eine Kopie der Datei, da bei Schlüsselverlust keine Möglichkeit mehr besteht, an die Daten zu gelangen. Wollen Sie darauf zugreifen, importieren Sie den Key vom Medium per Doppelklick. Das ist zwar umständlich, aber sicher.

Vergessen Sie nicht, das Zertifikat nach jeder Windows-Sitzung wieder von der Festplatte zu löschen, denn Windows legt den Zugangsschlüssel jedes Mal aufs Neue auf der Festplatte ab.

Automatische Backups durchführen

Komplette Datenträger sichern oder nur die Systemdateien – mit XP kein Problem. Das integrierte Backup-Programm ist über einen Assistenten einfach zu bedienen. Während Sie Ihre Windows-Partition sichern, können Sie ohne spürbare Performance-Einbußen weiterarbeiten. Ein Sicherungsauftrag lässt sich auch zeitgesteuert ausführen. Wer kein richtiges Backup fahren will, für den reicht die Systemwiederherstellung aus. Diese setzt nach einer Installation einen Wiederherstellungspunkt, zu dem Sie jederzeit zurückkehren können. Stört etwa der neue Grafikkartentreiber das System beim Hochfahren, lässt sich per Tastendruck die alte Konfiguration wiederherstellen.

Fazit: Sicher nur mit Updates

Das überraschende Ergebnis unseres Tests: Windows ist nicht so unsicher, wie viele glauben. Doch damit es so sicher wird, müssen Sie erst einmal rund 50 MByte Patches und Service Packs einspielen. Schade auch, dass gerade für die Hauptzielscheibe aller Virenautoren immer noch ein Virenscanner im Paket fehlt.

Wer sein System mit Updates auf dem neuesten Stand hält, automatische Backups fährt und sein Dateisystem verschlüsselt, ist mit XP auf der sicheren Seite. Nur bei der Benutzerverwaltung muss nachgebessert werden. fabian.vonkeudell@chip.de



SuSE Linux

Linux-User verlassen sich auf die Sicherheit ihres Systems, denn Viren und Würmer machten bislang keine Schlagzeilen. Doch ist das System wirklich sicher, oder gibt es bloß nicht genug Schädlinge, die für Wirbel sorgen?

■ Vorbildlich ist bei Linux die Unterscheidung zwischen User ohne weiterreichende Rechte und Administratoren – ein Erbe von Unix. Viren und Würmer können daher im Ernstfall nur auf die eingeschränkten Rechte eines normalen Users zugreifen, der Schaden bleibt begrenzt.

Sicherheit im Internet

Schon beim „nackten" SuSE Linux entdeckt der Online-Check von Qualys (siehe Kasten 53) deutlich weniger Lücken als bei Windows; die meisten in der niedrigsten Gefahrenstufe. Die Updates verändern diese Lückenstatistik allerdings nicht, erst wenn die integrierte Firewall manuell aktiviert wird, sind zehn weitere Lücken geschlossen. Trotzdem: fünf der untersten Gefahrenstufe bleiben übrig.

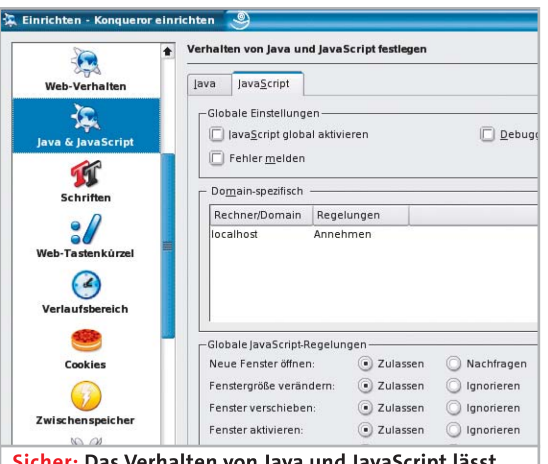
Sicherheits-Updates installieren

Wie bei Windows XP und MacOS X können die Updates über das Internet installiert werden. Der Haken: Nach der Installation ist das automatische Update deaktiviert, der Administrator muss es erst freischalten. Diese Einstellung können Sie ändern: Starten Sie Yast und aktivieren Sie im Modul »Software« die Option »Online-Update«. Wählen Sie im nächsten Fenster »Vollautomatisches Update konfigurieren« und setzen Sie einen Haken vor »Automatische Updates aktivieren«. Stellen Sie eine Uhrzeit für das tägliche Update ein, bestätigen Sie Ihre Eingaben, und das Auto-Update läuft.

Firewall einschalten & einrichten

Da die SuSE-Firewall nicht automatisch aktiviert wird, sollten Sie dies als erstes erledigen. Rufen Sie im Konfigurations-Manager Yast »Sicherheit und Benutzer« auf. Klicken Sie auf »Firewall« und wählen Sie die Netzwerk-Schnittstelle aus, die Sie schützen wollen. Bei einem Einzelplatzrechner mit DSL heißt das richtige Interface »dsl0«. Klicken Sie auf »Weiter« und lassen Sie alle Checkboxen frei. Wählen Sie nochmals »Weiter« und aktivieren Sie unter »Firewall-Features« nur den Eintrag »Alle laufenden Dienste schützen«.

Server-Betreiber sollten sich zusätzlich überlegen, Ping-Anfragen zu filtern. Dazu müssen Sie die Konfigurationsdatei SuSEFirewall2 im Verzeichnis »/etc/sysconfig« bearbeiten. Als Administrator „Root" öffnen Sie die Datei mit einem Editor und setzen den Wert der Variablen »FW_ALLOW_PING_FW« auf »no«. Damit verbieten Sie Ihrer Schutzmauer, auf Pings zu antworten.



Sicher: Das Verhalten von Java und JavaScript lässt sich im Konqueror bequem einstellen.

Browser konfigurieren

Die SuSE-Standard-Installation nimmt als Web-Browser Konqueror, der auch als Datei-Manager und FTP-Client →

arbeitet. Kurios: Unser Sicherheits-Check für Browser verweigert beim ersten Versuch seinen Dienst. Der Grund: Konqueror meldet sich als Netscape 5. Das können Sie über »Einstellungen | Konqueror einrichten/Browser-Identifizierung« ändern. Entfernen Sie das Häkchen vor »Kennung senden«.

Der Browser-Check fand beim Konquerer keine einzige Sicherheitslücke. Der Test auf Cross-Site-Scripting (erzwungene Umleitung per Skript auf andere Websites) wurde allerdings mit einer Fehlermeldung abgebrochen.

Java und JavaScript sind automatisch aktiviert. Wer darauf verzichten kann, schaltet das besser ab. Gehen Sie dazu in »Einstellungen | Konqueror | Java&Javascript« und entfernen Sie die Häkchen vor »Java global entfernen« und »Javascript global entfernen«. Die unsicheren Microsoft-Techniken ActiveX und VisualBasic-Script beherrscht der KDE-Browser nicht. Unser Tipp: Tauschen Sie den Standard-Browser gegen Mozilla Firefox aus, der ist genauso sicher, aber viel komfortabler.

Virenschutz aktivieren

Digitale Schädlinge sind unter Linux Nebensache. Der russische Sicherheits-Experte Eugene Kaspersky ist sich zwar sicher, dass dies nur an der eingeschränkten Verbreitung von Linux liegt. Stand der Dinge ist jedoch, dass es so gut wie keine bedrohlichen Linux-Viren gibt.

Ein Scanner fehlt zwar in der Standard-Installation, im Gegensatz zu Windows wird er aber zumindest mitgeliefert: Auf den SuSE-CDs oder -DVDs finden Sie AntiVir von H+BEDV. Geben Sie nach der Installation in einer Root-Shell den Befehl »antivir –update« ein. Die Software besorgt sich auf diese Weise die aktuellen Virensignaturen per Internet.

Sicherheit auf dem Rechner

Bei der SuSE-Installation müssen Sie neben einem Root-Account als Administrator auch mindestens einen normalen Benutzer festlegen. Wer sich auf der grafischen Oberfläche als „Admin“ anmeldet, bekommt zur Warnung einen knallroten Desktop präsentiert, der mit hochgehenden Bomben gespickt ist. Spätestens da ist klar: Es wird gefährlich! Denn als Administrator dürfen Sie unter Linux so ziemlich alles ändern. SuSE setzt die Trennung von Benutzer und Root strikt um, denn sobald ein normaler Anwender versucht, Änderungen am System vorzunehmen, fragt ein aufspringendes Fenster nach dem Root-Passwort.

Benutzerkonten sichern

Linux ist ein Mehrbenutzer-System, das bedeutet, alle Benutzer müssen sich explizit anmelden. Theoretisch zumindest, denn SuSE schaltet für den ersten angelegten Benutzer die automatische Anmeldung frei. Damit kommt jeder, der diesen Rechner einschaltet, an Ihre Daten – unsicherer geht es kaum. Deaktivieren Sie deshalb im Modul »Benutzer bearbeiten und anlegen« unter »Sicherheit und Benutzer« die automatische Anmeldung. Wählen Sie dazu den automatisch angelegten Benutzer aus und klicken Sie auf »Optionen für Experten«. Als nächstes drücken Sie auf »Einstellungen für das Anmelden«. Entfernen Sie jetzt den Haken vor »Automatische Anmeldung«. Auch »Anmeldung ohne Passwort« sollten Sie nicht aktivieren.

Passwörter verschlüsseln

Die Passwort-Sicherheit unter Linux hat sich bewährt: Passwörter werden mit einem Sicherheits-Algorithmus codiert und in der Datei »/etc/shadows« abgelegt, die nur für den Benutzer „Root“ lesbar ist. Auch SuSE bietet eine Passwort-Verschlüsselung: Öffnen Sie das Yast-Modul »Sicherheit und Benutzer« und gehen Sie ins Untermenü »Einstellungen zur Sicherheit«. Für Einzelplatzrechner mit Internetzugang ist die Sicherheitsstufe »Level 1« gedacht. Markieren Sie die entsprechende Checkbox und klicken Sie auf »Beenden«.



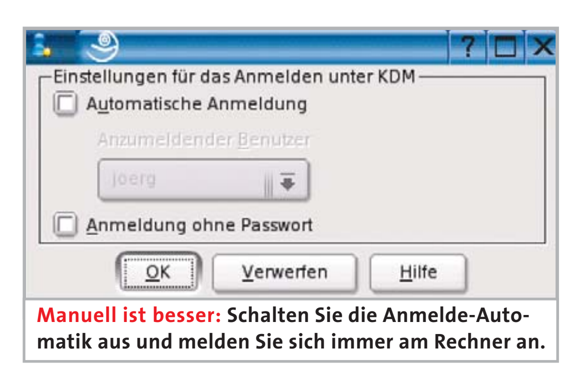
Unknackbar: Linux kann das Filesystem Ihrer Festplatte mit dem DSA-Algorithmus sichern.

Dateisystem codieren

Verschlüsselung gehört bei SuSE dazu. Schon bei der Installation lassen sich ganze Partitionen mit einem Krypto-Dateisystem ausstatten.

! ACHTUNG: Wenn Sie das Krypto-Filesystem einsetzen wollen, müssen Sie es schon bei der Installation explizit einschalten, denn nachträgliches Verschlüsseln wirkt wie neu formatieren und führt zu komplettem Datenverlust.

Dateien und Verzeichnisse können Sie unter KDE mit „KGpg“ (das Pendant zu PGP in der Windows-Welt) verschlüsseln. Im Kontextmenü des Konquerors wählen Sie unter »Aktionen« den Eintrag »Ordner packen und verschlüsseln« aus. Haben Sie noch kein Schlüsselpaar angelegt, werden Sie jetzt automatisch aufgefordert, dies zu tun. Ein Assistent führt Sie durch diesen Prozess. Wenn Sie zuvor schon gültige Keys erzeugt haben, können Sie diese über die Schlüsselverwaltung von „KGpg“ auswählen. Zum Entschlüsseln verwenden Sie einfach das Passwort, das Sie bei der Erzeugung der Schlüssel festgelegt haben. →



Manuell ist besser: Schalten Sie die Anmelde-Automatik aus und melden Sie sich immer am Rechner an.

Backups durchführen

Die Funktionen für Backup und Systemwiederherstellung finden Sie in Yast unter »System«. Der Backup-Assistent speichert die Systemdateien wahlweise lokal auf der Festplatte oder auf einem NFS-Server. Bei der Wiederherstellung müssen Sie nur die Backup-Datei auswählen, alles weitere erledigt das System. Vorbildlich: SuSE legt einmal am Tag automatisch eine Kopie der zentralen Konfigurations-Datei RC.CONFIG an.

Leider können Sie mit Yast automatische Backups nicht Ihren Wünschen anpassen. Wer sein System in regelmäßigen Abständen sichern will, muss einen Cron-Job anlegen. Cron-Jobs sind Prozesse, die automatisch vom System gestartet werden und beispielsweise tägliche oder wöchentliche Aufgaben definieren. Möchten Sie den Job täglich ausführen lassen, legen Sie ein Shell-Skript im Verzeichnis »/etc/cron.daily« ab. Es wird dann jeden Tag automatisch abgearbeitet. Wann das passiert, steht in der Datei »/etc/crontab«. Sie synchronisieren die tägliche Arbeit an einem Artikel per Cron-Job mit diesem Shell-Skript im Backup-Verzeichnis:

```
#!/bin/sh
#Backup·der Artikel·von·Joerg
rsync·–av·/home/joerg/artikel/
/backup/artikel/
```

Fazit: Sicher mit wenigen Tricks

Das gegenwärtige Dilemma von Linux: Es soll einfach genug sein, um Einsteiger in die Linux-Welt zu locken, und zugleich bombensicher. In SuSE geht der Komfort für den Nutzer an einigen Stellen zu weit, die Standard-Installation ist nicht perfekt abgesichert. Durch automatisches Login oder die Vorkonfiguration des SSH-Dienstes (sehr sicheres Kommandozeilen-Tool via Internet) entstehen Angriffspunkte auf ein sonst sicheres Betriebssystem. Ähnliches gilt für die ausgeschaltete Firewall. Bei den Updates dagegen fehlt es an Komfort, das Auto-Update muss erst freigeschaltet werden. Vorteil von SuSE: Die CDs enthalten alle nötigen Sicherheits-Tools. Auch die Wurm-Epidemie ist unter Linux kein Thema, das verhindert die vorbildliche Trennung von Administrator und gewöhlichem User.

joerg.geiger@chip.de



Apple-User sind sich einer Sache gewiss: OS X ist sicher. Schaut man sich unsere Testergebnisse an, dann sieht es ganz so aus. Doch in letzter Sekunde erreichte uns eine Nachricht, die schnelle Patches auch für Macianer notwendig macht.

MacOS X basiert auf „Darwin“, einem angepassten Unix. Bislang galt es als sicher, doch mit der Einführung von „Panther“ und dem neuen Kernel kann sich das ändern. Das Thema Viren spielt auf dem Mac kaum eine Rolle – etwa fünf Prozent Marktanteil machen das MacOS für Hacker uninteressant. Derzeit sind nur 30 Viren bekannt, die die Plattformen bis zur Version 9.2.2 angreifen.



Einfach: Wie bei den Mitkonkurrenten können Sie bei Apple Updates automatisch einspielen lassen.

Sicherheit im Internet

Macianer dürfen sich freuen: Schon in der ungepatchten Installation erkennt unser Lücken-Test (siehe 53) die wenigsten Lecks, alle in der niedrigsten Stufe. Nach dem Anpassen der Firewall bleiben nur noch zwei harmlose Lücken offen.

Sicherheits-Updates einspielen

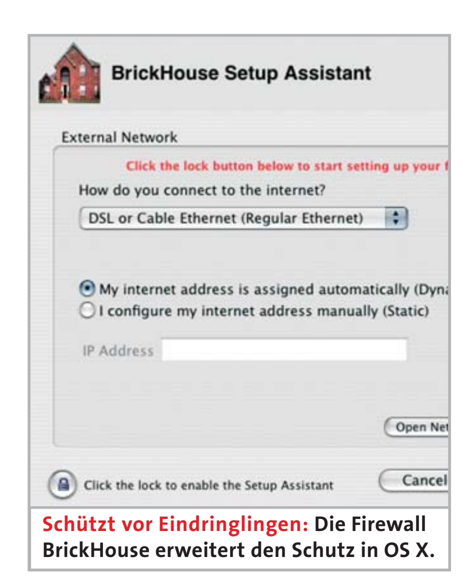
Wie schon Windows XP und SuSE Linux bietet MacOS X eine automatische »Software Aktualisierung«. Sie überprüft regelmäßig, ob auf den Apple-Servern Updates vorhanden sind. Diese können Sie direkt installieren oder nur speichern. Nicht benötigte Updates lassen sich ausblenden. Über die »Software Aktualisierung« installierte Updates werden in einer zentralen LOG-Datei verwaltet.

Firewall konfigurieren

Die Firewall ist automatisch aktiviert, das erklärt auch das gute Abschneiden beim ersten Test-Durchlauf. Leider lassen sich über »Firewall« kaum Einstellungen vornehmen: Sie können die vordefinierten Firewall-Regeln nicht weiter anpassen und auch nicht durch eigene Regeln die Dienste auf bestimmten Rechnern und Netzwerken einschränken. Außerdem bleiben alle UDP-Ports außen vor. Schade, denn ein BSD-Paketfilter für TCP, UDP, ICMP und IGMP (siehe Glossar auf 54) ist mit „ipfw“ in MacOS X schon enthalten. Offensichtlich will Apple seinen Kunden aber nur eine einfach zu konfigurierende Firewall anbieten, die beim Starten von Diensten wie „Apple File Sharing“ und „Windows Sharing“ automatisch Zugriff gewährt.

Um auch ipfw einfach konfigurieren zu können, brauchen Sie die Shareware Brick-House (**http://personalpages.tds.net/~brian_hill/brickhouse.html**). Damit schließen Sie vier der sechs von Qualys gefundenen Sicherheitslücken. So geht’s: Nach dem Start führt Sie ein Assistent durchs Procedere. Sie müssen sich durch Klicken auf das „Schloss“ als Administrator identifizieren. Legen Sie Ihre Internetverbindung (Ethernet, DSL-Modem, normales Modem) und die Art fest, wie Sie Ihre IP beziehen. Meist geschieht dies dynamisch durch den Provider. Überspringen Sie die folgenden Dialogfelder und klicken Sie zum Abschluss auf »Done«.

Sie können nun die Firewall aktivieren und Regeln hinzufügen, etwa um die beiden noch offenen Ports 514 und 1434 zu schließen. Klicken Sie dazu auf »Add Filter« und fügen Sie als »Deny«-Regel für eingehende Verbindungen den UDP-Port 514 hinzu. Gleiches gilt für Port 1434. Um das System vor Ping- und Traceroute- →



Schützt vor Eindringlingen: Die Firewall BrickHouse erweitert den Schutz in OS X.

Anfragen zu schützen, müssen Sie die Regeln anpassen. Klicken Sie auf »Advanced« und deaktivieren Sie »Allow All ICMP Traffic« sowie »Allow FTP Data Port«. Auch »Allow Network Time« deaktivieren Sie. Bedenken Sie aber, dass Anpassungen im ICMP-Bereich, je nach Provider, Probleme bei der Einwahl verursachen können. Um die Einstellungen festzulegen, klicken Sie auf »Apply«, dann auf »Install« und danach auf »Save«.

Internet-Browser sichern

Apple liefert mit OS X den Browser „Safari" aus, Microsofts Internet Explorer wird nicht mehr installiert. Prinzipiell setzt Apple auf strikte Deaktivierung aller gefährlichen Dienste und gibt diese nur frei, wenn der User explizit zustimmt. Da ActiveX unter MacOS ohnehin kein Thema ist, sollten Sie in Safari unter »Sicherheit« noch Java und JavaScript deaktivieren. Im Browser-Test haben wir Safari mit Standardeinstellungen dem Online-Check unterzogen. Ergebnis: keine Lücke – zumindest war das bis Mai 2004 so. Seither sind gravierende Lücken entdeckt worden. Was Sie dagegen tun können, steht im Kasten rechts.

Virenschutz einrichten

Ist OS X sicher vor Viren, Würmern und Trojanern? Noch ja. Doch am 8. April 2004 machte die Sicherheitsfirma Intego auf eine Gefahr aufmerksam: Das Unternehmen gab an, dass ein Programmierer zu Testzwecken den Trojaner „MP3Concept" entwickelt habe. Mit i-Tunes, Apples Jukebox, richtet die infizierte Datei keinen Schaden an. Öffnet man sie aber im »Finder«, startet der Virus einen fingierten Angriff. Bei ihm handelt es sich um ein „Proof of Concept" – Schäden bleiben also aus. Das Beispiel zeigt aber, dass auch OS X in Gefahr ist.

Einzig Makro-Viren sind ein Thema: Sie können auch bei „Office:mac" Schaden anrichten. Aktivieren Sie einfach den Makroschutz in Word und Co. Sollten Sie für Ihren Apple tatsächlich einen Virenscanner kaufen wollen, bietet sich VirusBarrier von Intego an. Mehr Infos unter **www.intego.com/virusbarrier**.

Sicherheit auf dem Rechner

Lokale Anmelde-Kennwörter zurückzusetzen ist bei OS X leider noch simpler als bei Windows XP: Installations-CD rein, Rechner neu starten und die [C]-Taste gedrückt halten. Schon kann ein böswilliger Kollege alle Kennwörter zurücksetzen.

Firmware-Passwort setzen

Richten Sie deshalb ein Firmware-Passwort (quasi ein BIOS-Passwort) ein. Voraussetzung: Ihr Rechner verfügt über die aktuelle Firmware (ab 4.1.7). Um das zu prüfen, klicken Sie im »Apfel«-Menü auf »Über diesen Mac«, dann auf »weitere Informationen«, um den »System-Profiler« zu starten. In der Hardware-Übersicht steht die Firmware-Version unter »Boot-ROM-Version«. Legen Sie nun die erste Installations-CD ein und wechseln Sie in das Verzeichnis »Applications/Utilities«, starten Sie das Tool Open Firmware Password und klicken Sie auf »Ändern«. Nachdem Sie sich mit Ihrem Administrator-Passwort authentifiziert haben, aktivieren Sie »Ein Kennwort verlangen« und geben ein Firmware-Kennwort ein.

Sichere Kennwörter verwenden

Lokale Passwörter speicherte MacOS X bis zur Version 10.2 im Verzeichnisdienst Netinfo. Über diesen war das Knacken von Passwörtern recht einfach. Seit Version 10.3 legt OS X Passwörter ausschließlich als „Shadow-Passwort" ab, sie sind nur noch in Sternchen sichtbar. Ein Auslesen über den Befehl »nidump passwd.« ist also nicht mehr möglich. In 10.3 sind Passwörter mit mehr als acht Stellen erlaubt. Systeme, die von 10.2 auf die aktuelle Version gepatcht wurden, können noch alte gehashte Passwörter enthalten. Überprüfen Sie dies ebenfalls mit »nidump passwd.«. Sollten Sie gehashte Einträge finden, ändern Sie alle Passwörter in der Systemeinstellung »Benutzer«.

Benutzerverwaltung absichern

OS X trennt die Rechtevergabe in drei Nutzertypen auf: „Standard-Benutzer" „Administratoren" und „Root". Standard-Benutzer lassen sich mit individuellen Einschränkungen versehen und können Home-Verzeichnisse anderer User nicht lesen oder löschen. Administratoren können keine Systemdateien löschen, das bleibt dem „Root" vorbehalten. Die Benutzerverwaltung ist damit mindestens genauso sicher wie unter Linux. Der erste User, den Sie bei der Installation anlegen, ist automatisch Administrator. Die Benutzerverwaltung wird zentral über die Systemeinstellung »Benutzer« vorgenommen. Sollte das Schloss-Symbol geschlossen sein, melden Sie sich als Admin an. Damit aber ein lokaler Angreifer erst gar nicht sieht, welche User auf dem System angelegt sind, schalten Sie auf alle Fälle die automatische Anmeldung ab: Klicken Sie auf »Anmelde-Optionen«, deaktivieren Sie die automatische Anmeldung und →

IN LETZTER SEKUNDE

» Neue Lücke in OS X

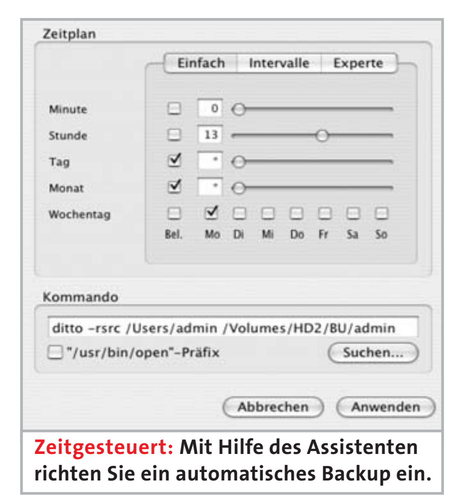
Nach Abschluss unseres Tests wurde eine gravierende Sicherheitslücke in OS X entdeckt, die neben Safari auch alle anderen Browser unter OS X betrifft. Durch sie kann ein Angreifer über eine „präparierte" URL im Hintergrund ein Disk-Image laden, das beispielsweise über ein Skript das komplette Home-Verzeichnis löscht, ohne dass es der User bemerkt. Apple hat zwar einen Patch bereitgestellt, der behebt aber nicht alle Probleme. Wirklich sicher sind Sie nur mit dem Tool „Paranoid Android". Diese Freeware schützt auch vor dem so genannten HelpViewer, der ähnliche Probleme macht.
Weitere Infos dazu finden Sie unter: **www.unsanity.com/haxies/pa**

ändern Sie das Anmeldedialogfeld auf »Name und Kennwort«. Auch die Optionen »Ruhezustand«, »Neustart« und »Ausschalten« deaktivieren Sie. Dies verhindert, den Rechner aus dem Anmeldestatus heraus neu zu starten. Weitere Einstellungen nehmen Sie unter »Systemeinstellung | Sicherheit« vor. Schalten Sie dort den Kennwortschutz für den Bildschirmschoner und den Admin-Zugriff für alle Systemeinstellungen an und erzwingen Sie somit bei Inaktivität die automatische Abmeldung vom System.

Dateien und Ordner verschlüsseln

Zum Verschlüsseln von Dateien, liefert OS X das Verfahren OpenSSL mit. Damit Sie leichter arbeiten können, setzen Sie die Shareware „PuzzlePalace“ (**http://personalpages.tds.net/~brian_hill/puzzlepalace.html**) ein. Damit konfigurieren Sie die als sicher geltenden Verschlüsselungs-Algorithmen Blowfish Cipher, Triple DES, DEA, CAST oder RC5. Wählen Sie eine Methode, ziehen Sie die gewünschte Datei auf das geöffnete Programm und vergeben Sie ein Kennwort.

Für mobile Zeitgenossen ist »File Vault« unter »Systemeinstellung | Sicherheit« optimal. Das Tresor-Symbol steht für die 128-Bit-Verschlüsselung des Home-Verzeichnisses. Bei der Anmeldung eines berechtigten Users wird das verschlüsselte Home-Verzeichnis geöffnet und steht für die Dauer der Session bereit. Andere angemeldete User haben keinen Zugriff auf diesen Bereich. Bevor Sie FileVault nutzen können, müssen Sie das Haupt-Kennwort setzen. Danach aktivieren Sie FileVault, das Home-Verzeichnis wird automatisch verschlüsselt. Das Kopieren großer Datenmengen aus dem Home-Verzeichnis kann wegen der Verschlüsselung lange dauern.



Zeitgesteuert: Mit Hilfe des Assistenten richten Sie ein automatisches Backup ein.

Automatische Backups anlegen

In OS X gibt es kein Tool, das automatische Sicherungen erzeugt. Sie können aber einen Cron-Job einrichten, der zeitgesteuert Befehle ausführt. Dazu eignet sich die Freeware CronX 2.1. Nach dem Start klicken Sie in der Titelleiste auf »Neu«. Wählen Sie »Einfach« und legen Sie unter »Minute«, »Stunde« und »Wochentag« den Startzeitpunkt fest. Starten Sie das Backup mit »ditto –rsrc /Users/admin/Volumes/HD2/BU/admin«. Damit wird das Home-Verzeichnis des Users „admin“ auf die Partition HD2 im Verzeichnis BU gesichert.

Backups verschlüsseln

Das „Festplatten Dienstprogramm“ sichert Festplatten, Partitionen, Verzeichnisse und Dateien in ein Image. Vorteil: Das Image lässt sich mit 128 Bit verschlüsseln. Starten Sie das Tool unter »/Programme/Dienstprogramme«. Wählen Sie »Images | Neu | Image von Ordner«. Über den Datei-Browser markieren Sie nun das zu sichernde Verzeichnis und drücken auf »Öffnen«. Vergeben Sie einen Namen und legen Sie den Speicherort fest. Nun aktivieren Sie das gewünschte Image-Format und die Verschlüsselung. Klicken Sie auf »Sichern«, und der Vorgang startet. Das Image lässt sich via Doppelklick als Laufwerk einbinden.

Fazit: Bis jetzt sehr sicher

Im Rohzustand ist OS X von außen kaum angreifbar. Im lokalen Bereich hingegen stehen die Tore offen. Schade, dass Apple hier zu wenig tut, um seine Kunden über Schutzmaßnahmen zu informieren. Denn mit wenig Aufwand lassen sich die meisten Sicherheitslöcher stopfen. Dafür liefert Apple das neue MacOS X „Panther“ mit sinnvollen Sicherheits-Features aus, darunter Software aus der Open-Source-Szene. Wer noch mehr Sicherheit will, spielt ein paar Freeware- oder Shareware-Tools ein. Profi müssen Sie also nicht sein, Unix-Kenntnisse sind jedoch vorteilhaft.

Daniel Schmid, autor@chip.de

GESAMT-FAZIT



Windows, Linux, Apple: Welches OS ist das sicherste?

Sind Sie auch der Meinung, dass Windows total unsicher ist? So denken viele – und täuschen sich. Die große Überraschung unseres Tests: Das viel geschmähte Microsoft-Betriebssystem hat gezeigt, dass es besser ist als sein Ruf. Allerdings – und das relativiert unser Ergebnis wieder – braucht es dazu jede Menge Patches und das aktuelle Service Pack 2. Ohne diese zeigt Windows nicht nur die meisten, sondern auch die schlimmsten Sicherheitslücken; nach den Updates sind aber alle geschlossen. Linux und Apple sind zwar von Haus aus weniger anfällig, dafür bleiben nach den Updates noch kleinere Lücken offen.

Wo also liegen die Unterschiede? Geht es um Viren, Würmer und Trojaner, kommt Windows XP derzeit am schlechtesten weg. Der Grund: Das System bringt keinen Virenscanner mit und ist wegen seiner Verbreitung (auf Desktop-Systemen rund 90 Prozent) das primäre Angriffsziel von Hackern.

Auch bei der lokalen Sicherheit schwächelt Windows. Denn in diesem Bereich ist es kaum konfigurierbar. Anders bei MacOS und SuSE Linux: Zwar ist dazu bei beiden Handarbeit nötig, danach sind sie aber deutlich besser gegen lokale Angriffe geschützt. Zusätzlichen Schutz verschafft ein verschlüsselbares Dateisystem, das aber nur Linux bietet. Apple und Windows können ohne zusätzliche Software nur Ordner und einzelne Dateien verschlüsseln.

Alle drei Systeme überzeugen mit Update-Routinen. Damit halten Sie Ihr System immer auf dem neuesten Stand. Im Falle von Windows ist das auch dringend nötig, denn das System aus Redmond bleibt Hauptziel aller Hacker. Aber auch Apple gibt Anlass zur Sorge: Die jüngst entdeckten Sicherheitslücken sind gravierend, hier wäre ein schneller Patch nötig gewesen. Apple und Microsoft (nur mit Service Pack 2) setzen inzwischen auf eine standardmäßig aktivierte Firewall, bei SuSE Linux muss sie erst manuell aktiviert werden.